IEEE P802.11
Wireless LANs

|  |
| --- |
| OCV with OCT |
| Date: 2019-01-11 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Thomas Derham | Broadcom | 16340 W Bernardo Dr, San Diego CA 92127 |  | thomas.derham@broadcom.com |
| Nehru Bhandaru | Broadcom | 250 Innovation Drive, San Jose CA 95134 | +1 408 922 5924 | nehru.bhandaru@broadcom.com |
| Laurent Cariou | Intel |  |  |  |
| Carlos Cordeiro | Intel |  |  |  |

Abstract

Operation Channel Validation was introduced in 11-17/1807r12 and 11-18/1353r2 to provide hardening against possible channel-based man-in-the-middle attacks. OCI information is included in relevant frames, including certain management frames, e.g. (Re)Association Request/Response for FT and FILS Authentication. It has been noted that OCV validation in the case that those management frames are sent using On-Channel Tunneling (i.e. via other STAs of a multiband device) is unclear/insufficient, because the frames might be sent over a different channel to the (expected or current) operating channel between the two STAs. This document proposes additional text for OCV to support this case.

Optional fields are added to OCI element/subelement so that both the expected/current operating channel between the two STAs, as well as the channel used to send/receive OCT tunneled frames, are specified when frames are sent over OCT. Rules on validation for this case are added. (These fields are not added to OCI KDE, since this is only used in EAPOL-Key frames which are not MMPDUs and so not sent over OCT).

In addition, although this is not directly related to OCV, this contribution proposes additional text regarding use of OCT procedure to send robust Management frames. A minimum time spacing is specified between transmission of two robust Management frames when one is sent using OCT and the other is sent over-the-WM, in order to minimize the possibility of out-of-order reception (due to difference in channel access delay between OCT and over-the-WM) resulting in replay counter mismatch. In addition, an AP is prevented from initiating an OCT exchange when Over-the-WM enabled (since the non-AP STA will, in general, not be listening on the OCT channel), and definitions of Over-the-WM enabled/disabled are clarified.

Changelog

r1 – editorial formatting improvements as suggested by the Editor

r2 – added text on OCT behavior when sending robust mgmt frames

**Instructions to the editor**

***Instruct the editor to modify Section 12.2.9 as follows:***

**12.2.9 Requirements for Operating Channel Validation**

When OCVC capability is present, a STA shall advertise this capability in RSNE and shall include operating channel information and validate the Operating Channel Information (OCI) received from an OCVC capable peer in certain protected messages used for key establishment and confirmation.

A STA with OCVC capability validates that the channel information in received OCI matches its current operating channel parameters by:

* Verifying that the maximum bandwidth used by the STA to transmit or receive PPDUs to/from the peer STA from which the OCI was received is no greater than the bandwidth of the operating class specified in the Operating Class field of the received OCI
* Verifying that the primary channel used by the STA to transmit or receive PPDUs to/from the peer STA from which the OCI was received is equal to the Primary Channel Number field (for the corresponding operating class)
* Verifying that, when 40 MHz bandwidth is used by the STA to transmit or receive PPDUs to/from the peer STA from which the OCI was received, the non-primary 20 MHz used matches the operating class (i.e. upper/lower behavior) specified in the Operating Class field of the received OCI
* Verifying that, if operating an 80+80 operating class, the frequency segment 1 channel number used by the STA to transmit or receive PPDUs to/from the peer STA from which the OCI was received is equal to the Frequency Segment 1 Channel Number field of the OCI.

If the NT-MLME of a STA with OCVC capability processes an MMPDU containing OCI received in an MLME-OCTunnel.indication primitive (see section 11.32.5 On-channel Tunneling (OCT) operation):

* The above validation is performed with respect to the expected or current channel used by the STA to transmit or receive PPDUs to/from the peer STA directly over-the-WM, and
* In addition, the STA verifies that the OCI contains the OCT Operating Class, OCT Primary Channel Number and OCT Frequency Segment 1 Channel Number fields, and uses the OCT information in those fields to perform the above validation with respect to the channel used by the STA corresponding to the TR-MLME from which the MLME-OCTunnel.indication primitive was received to transmit or receive PPDUs containing On-channel Tunnel Request frames to/from the STA corresponding to the TR-MLME used by the peer STA.

If a STA with OCVC capability receives a frame from a peer STA which is not on the same primary channel (or frequency segment 1 channel number) used by the STA to receive PPDUs from the peer STA, or has bandwidth that exceeds the maximum bandwidth used by the STA to receive PPDUs from the peer STA, the frame is discarded.

***Instruct the editor to add the following paragraph to the end of Section 11.32.5 On-Channel Tunneling Operation:***

If the NT-MLME of a STA sends a robust Management frame with a given AC using the OCT procedure to the NT-MLME of a peer STA, the STA shall wait for at least 20 TUs after the reception of the corresponding MLME-OCTunnel.confirm primitive before sending another robust Management frame with the same AC over-the-WM (i.e., not using the OCT procedure) to the same peer STA.

The MLME of an AP shall not use the OCT procedure to communicate with the MLME of a non-AP STA while those MLMEs are over-the-WM enabled. A pair of MLMEs become over-the-WM enabled once they are able to perform a successful frame exchange directly over the air (i.e., without using the OCT procedure). A pair of MLMEs become over-the-WM disabled once either of the MLMEs no longer operates on the same channel (e.g. in case one of the MLMEs switches operating channel) or once one of the MLMEs receives a frame from the peer MLME using the OCT procedure.

***Instruct the editor to modify* 9.4.2.236 as follows:**

9.4.2.236 OCI Element

The OCI element is shown in Figure TBD (OCI element format)

The Element ID and Length fields are defined in 9.4.2.1 (General)

The Operating Class field is set to the global operating class that corresponds to the widest bandwidth currently being used by the transmitting STA. See Annex E, Table E-4 for description of the global operating classes.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Element ID | Length | Element ID Extension  | Operating Class | Primary Channel Number  | Frequency Segment 1Channel Number | OCT Operating Class (optional) | OCT Primary Channel Number (optional) | OCT Frequency Segment 1Channel Number (optional) |

Octets: 1 1 1 1 1 1 0 or 1 0 or 1 0 or 1

**Figure 9-762 OCI element format**

The Primary Channel Number field is set to the primary channel being used currently. Primary Channel Number is one of the channels from the row corresponding to the operating class as defined in Annex E or the primary 20 MHz (sub)channel allowed for HT or non-HT operation for operating classes that specify only channel center frequency indices.

The Frequency Segment 1 Channel Number field is set to the channel center frequency index of the secondary segment (frequency segment 1) being used currently, if applicable, or set to 0 otherwise. Frequency Segment 1 Channel Number is one of the center frequency indices from the row corresponding to the operating class as defined in Annex E.

The OCT Operating Class, OCT Primary Channel Number and OCT Frequency Segment 1 fields are present if the OCI element is contained in a frame sent using On-channel tunneling, i.e. an MMPDU included in an MLME-OCTunnel.request or MLME-OCTunnel.response primitive (see 11.32.5 On-channel Tunneling (OCT) operation); otherwise they are not present. They have the same definition as the Operating Class, Primary Channel Number and Frequency Segment 1 fields, except that they pertain to the channel used by the STAs corresponding to the TR-MLMEs to transmit and receive PPDUs containing On-channel Tunnel Request frames.

***Instruct the editor to modify the following description for the FT OCI subelement in 9.4.2.47***

The OCI subelement contains the operating channel information which is integrity protected (see procedures in 13.78 (FT reassociation)) as defined in Figure 9-359 (OCI subelement format)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Subelement ID | Length | Operating Class | Primary Channel Number | Frequency Segment 1 Channel Number | OCT Operating Class (optional) | OCT Primary Channel Number (optional) | OCT Frequency Segment 1Channel Number (optional) |

Octets: 1 1 1 1 1 0 or 1 0 or 1 0 or 1

The definitions of Operating Class, Primary Channel Number, ~~and~~ Frequency Segment 1 Channel Number, OCT Operating Class, OCT Primary Channel Number and OCT Frequency Segment 1 Channel Number fields are the same as those described in section 9.4.2.236 OCI Element.